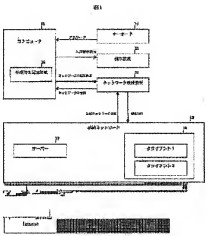
INFORMATION PROCESSOR AND START CONTROLLING METHOD

Publication number: JP2002278932 (A)
Publication date: 2002-09-27
Inventor(s): ARAKAWA TENKO +
Applicant(s): HITACHI LTD +
Classification:
- international: ***G06F12/14; G06F15/00; G06F21/20; G06F21/24; G06F12/14; G06F15/00; G06F21/00; G06F21/20;*** (IPC1-7): G06F12/14; G06F15/00
- European:
Application number: JP20010081861 20010322
Priority number(s): JP20010081861 20010322

Also published as:
JP3975685 (B2)

Abstract of JP 2002278932 (A)
PROBLEM TO BE SOLVED: To provide an information processor for preventing the leakage of data in the information processor and improving convenience by using connection information of a network. SOLUTION: Peculiar information of a server on the network to be used is recorded in the information processor having a network connection device. When power is supplied and is restored, network information is read and compared. When the state of the server changes and the server cannot be detected, authentication is performed by using a method other than network information. Thus, a person except for a user is prevented from using the processor. In a regular network connection environment, the information processor can be used even if the user does not perform authentication work.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－278932
（P2002－278932A）
(43)公開日　平成14年９月27日(2002.9.27)

(51)Int.Cl.'	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０１７
			３３０Ｃ	５Ｂ０８５
12/14	３２０	12/14	３２０Ａ	

審査請求　未請求　請求項の数２　ＯＬ　（全４頁）

(21)出願番号　特願2001－81861(P2001－81861)

(22)出願日　平成13年３月22日(2001.3.22)

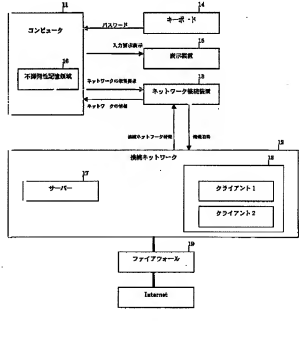
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　荒川　天広
神奈川県海老名市下今泉810番地　株式会社日立製作所インターネットプラットフォーム事業部内
(74)代理人　100075096
弁理士　作田　康夫

Ｆターム(参考)　５Ｂ０１７　ＡＡ０３　ＢＡ０９
５Ｂ０８５　ＡＡ０８　ＡＣ０２　ＡＥＤ１

(54)【発明の名称】　情報処理装置および起動制御方法

(57)【要約】
【課題】ネットワークの接続情報を利用して、情報処理装置のデータ漏洩防止と、利便性の向上を実現する情報処理装置を提供する。
【解決手段】ネットワーク接続装置を持つ情報処理装置に、使用するネットワーク上のサーバーの固有情報を記録しておき、電源投入時や復電時においてネットワーク情報を読み取り比較する。サーバーの状態が変化した時や、サーバーが見つからない場合には、ネットワーク情報以外の手法を用いて認証を行うことで使用者本人以外が使用できないようにするが、通常のネットワーク接続環境においては使用者が認証作業を行わなくても情報処理装置が使用可能になることを特徴としている。

図1



【特許請求の範囲】

【請求項１】ネットワークへの接続が可能な情報処理装置において、少なくとも接続するサーバー名称とサーバーのMACアドレスを含むネットワーク接続情報をあらかじめ記憶する接続情報記憶部と、前記接続情報記憶部のネットワーク接続情報を基にネットワークへの再接続可否を判定する接続判定部と、前記接続判定部の結果に基づき、情報処理装置のシステム起動や節電状態からの復帰を制御する起動制御部とを備え、前記接続判定部が記憶するネットワーク接続情報でネットワークに再接続できなかった時に、前記起動制御部は、ユーザ認証をおこなうことを特徴とする情報処理装置。

【請求項２】ネットワークへの接続が可能な情報処理装置の起動制御方法において、接続するサーバー名称とサーバーのMACアドレスを接続情報記憶部に記憶し、情報処理装置の起動時あるいは節電状態からの復帰時に、ネットワークから前記サーバー名称に対応する該サーバーのMACアドレスを取得し、前記ネットワークから取得したMACアドレスと前記接続情報記憶部のサーバーのMACアドレスを比較し、一致したときには、情報処理装置の起動あるいは節電状態からの復帰を継続し、不一致のときには、ユーザ認証をおこなうことを特徴とする起動制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置の起動方法に係り、特に通常はネットワークに接続して利用される情報処理装置の起動方法に関する。

【０００２】

【従来の技術】情報処理装置の不正利用やデータの漏洩を防止する方法として、情報処理装置の起動時または復電時にユーザ認証を実行することが広く行われている。ユーザ認証データ入力方法としては、キーボードからパスワードを入力させるのが最も一般的である。これ以外に指紋や声紋等を利用した認証方法も採用され始めている。

【０００３】

【発明が解決しようとする課題】しかしながら、上記の従来の方法ではユーザ認証データ（パスワード）を設定し、起動や復電のたびに、パスワード入力しなければならない。このため、入力の手間がかかり、操作性が悪い。このため、パスワード設定をおこなわない場合も多く、この場合には、情報処理装置を盗まれたときにデータの保護ができないという問題があった。これを解決するために物理的なキーを用いる方法が考案された。しかし、物理的なキーを用いた場合には、キーの携帯が必要な上に、製造コストの上昇や、キーを情報処理装置と同時に盗まれた場合にデータを保護できないという問題があった。

【０００４】本発明は、上記従来の問題点を解決し、操作性がよく信頼性の高い情報処理装置を提供するものである。つまり、認証用の物理的な装置が不要としたことにより製造コストの上昇も無く、コンピュータの盗難時においてもデータの保護が可能な、第三者による不正利用の防止とユーザの利便性の向上が可能な情報処理装置を提供するものである。

【０００５】

【課題を解決するための手段】上記課題を解決するために、本発明の情報処理装置は、通常使用時にはネットワークに接続され、盗難時には異なる場所で使用されるために、ネットワークに接続されていないか、異なるネットワークに接続されることに着目した。

【０００６】よりくわしくは、通常使用時に接続しているネットワークのネットワーク接続情報を接続情報記憶部に記憶しておく。例えば、前記ネットワーク情報は、接続するサーバー名称と該サーバーのMACアドレスとする。情報処理装置のシステム再起動時や節電状態からの復帰時に、前記接続情報記憶部のネットワーク情報を基にネットワークの再接続可否を判定する。例えば、サーバー名称に対応するサーバーのMACアドレスを接続するネットワークから取得し、前記接続情報記憶部の該サーバーのMACアドレスと比較し、一致するときには、ネットワークに再接続可能と判断する。ネットワークへ再接続可能な場合には、システム起動あるいは節電状態からの復帰を継続し、不一致のときには、キーボードからパスワードを入力する方法等のユーザ認証をおこなうようにする。

【０００７】

【発明の実施の形態】この発明の一実施形態を、図面を参照しながら説明する。図１において、コンピュータ１１は不揮発性記憶領域１６を持ち、ネットワーク接続装置１３、キーボード１４、表示装置１５、ネットワーク接続装置１３を経由して接続ネットワーク１２に繋がっている。接続ネットワーク１２には、サーバー１７及びクライアント１８があり、外部のネットワークからはファイアウォール１９により防護されている。以上のように構成されたシステムにおけるユーザ認証方法について、図１、図２を用いてその動作を説明する。

【０００８】通常使用時に、コンピュータ１１上のパスワードと、接続ネットワーク１２中においてコンピュータ１１がアクセスを行うサーバー１７のサーバー名とサーバー１７に割り付けられたMACアドレスをコンピュータ１１内の不揮発性記憶領域１６に登録する。

【０００９】コンピュータ１１は、電源投入時や節電状態からの復帰時に、不揮発性記憶領域１６からサーバー名を読み出し、ネットワーク接続装置１３を使用して接続ネットワーク１２内にあるサーバー１７を検索する。サーバー１７が存在する場合にはサーバー１７のMACアドレスを読み取り、不揮発性記憶領域１６に登録したMACアドレスと比較する（ステップ２２）。サーバー１７

から読み出したMACアドレスと不揮発性記憶領域１６に登録したMACアドレスと同一な場合にはユーザ認証を完了し、コンピュータ１１を使用可能な状態とする（ステップ２５）。

【００１０】サーバー１７から読み出したMACアドレスが不一致の場合や、接続ネットワーク１２内にサーバー１７が発見できない場合には接続ネットワーク１２の情報を使用しない認証作業へ移る。表示装置１５によりユーザに対して認証作業を促す表示を行い、キーボード１４によるパスワード入力による認証を行う（ステップ２３、ステップ２４）。

【００１１】ユーザ認証が完了した場合には、コンピュータ１１を使用可能な状態にする（ステップ２５）。認証作業が正しく行われない場合にはコンピュータ１１を使用不可能な状態とする（ステップ２６、ステップ２７）。

【００１２】このように図２に示す一連の認証作業は、コンピュータが起動される場合や、省電力状態からの復帰時や、ネットワークへのログインを行う際にBIOS、あるいはOSの起動処理やログインプロセスで実行されるタスクやドライバで処理を行う。

【００１３】

【発明の効果】以上説明したように、本発明はネットワークへの接続装置を持つコンピュータが、ネットワーク上の接続サーバーのネットワーク情報を利用することで、通常の使用環境での個人認証を省略可能になり、操作性が向上する。また、コンピュータが第３者の手に渡った場合には、使用者を特定できた場合のみ使用可能としているために、データの漏洩を防止することが可能である。

【図面の簡単な説明】

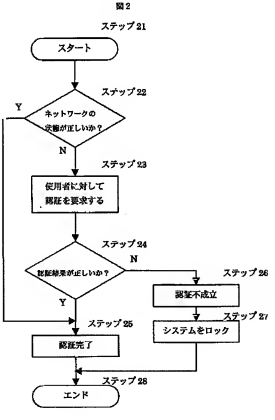
【図１】本発明の一実施形態を示す図である。

【図２】本発明による認証方法を説明するためのフローチャートである。

【符号の説明】

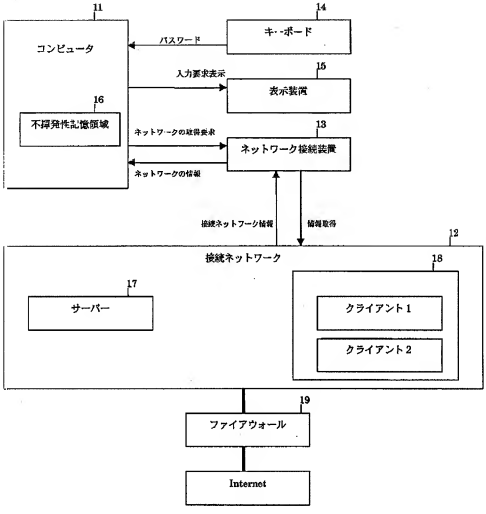
１１　コンピュータ
１２　接続ネットワーク
１３　ネットワーク接続装置
１４　キーボード
１５　表示装置
１６　不揮発性記憶領域
１７　サーバー
１８　クライアント
１９　ファイアウォール

【図２】



【図1】

図1


11
コンピュータ
16
不揮発性記憶領域
パスワード
14
キーボード
入力要求表示
15
表示装置
ネットワークの接続要求
ネットワークの接続
13
ネットワーク接続装置
接続ネットワーク接続
接続取得
12
接続ネットワーク
17
サーバー
18
クライアント1
クライアント2
19
ファイアウォール
Internet